

AFTER FINAL GROUP ART 2135REMARKS

The application was filed on 19 April 2001 with sixteen claims. The Examiner examined the application and on 21 October 2004 issued a first Action. In the Examiner's Action, the Examiner rejected claims 1-7 and 10-16 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,405,364 B1 entitled BUILDING TECHNIQUES IN A DEVELOPMENT ARCHITECTURE FRAMEWORK to Bowman-Amuah (Bowman-Amuah '364). The Examiner also rejected claims 8-9 under 35 U.S.C. §103(a) as being unpatentable over Bowman-Amuah '364 in view of U.S. Patent No. 5,519,778 entitled METHOD FOR ENABLING USERS OF A CRYPTOSYSTEM TO GENERATE AND USE A PRIVATE PAIR KEY FOR ENCRYPTING COMMUNICATIONS BETWEEN THE USERS to Leighton et al. (Leighton '778). In response, Applicants amended the specification and claims. The Examiner then finally rejected claims 1-7 and 10-16 under 35 U.S.C. §103(a) as being unpatentable over Bowman-Amuah '364 in view of U.S. Patent No. 4,672,572 entitled PROTECTOR SYSTEM FOR COMPUTER ACCESS AND USE to Alsberg (Alsberg '572); and finally rejected claims 8 and 9 under 35 U.S.C. §103(a) over Bowman-Amuah '364, Alsberg '572, and Leighton '778. Applicants attempted to put the claims in condition for allowance and/or better condition for appeal by amendment. The Examiner did not enter the amendments. Applicants, believing that patentable subject matter exists, filed a Request for Continued Examination.

The Examiner then entered the amendments and rejected claims 1-7 and 10-16 under 35 U.S.C. §103(a) over Bowman-Amuah '364, Alsberg '572 and U.S. Patent No. 6,671,809B1 entitled SOFTWARE-DEFINED COMMUNICATIONS SYSTEM EXECUTION CONTROL to Perona et al. (Perona '809). The Examiner further maintained the same rejection of claims 8-9 under 35 U.S.C. §103(a) over Bowman-Amuah '364, Alsberg '572, and Leighton '778. Applicants amended the claims. The Examiner then issued a final rejection of the claims rejecting claim 7 under 35 U.S.C. §101, and claims 1-7 and 10-16 under 35 U.S.C. §103(a) over Bowman-Amuah '364 in view of Alsberg '572 and Perona '809. The Examiner maintained the rejection of claims 8-9 under 35 U.S.C. §103(a) over Bowman-Amuah '364, Alsberg '572, and Leighton '778.

AFTER FINAL GROUP ART 2135

The application has two independent claims: claim 1 is addressed to the methodology framework having five systems for designing a secure system. Claim 7 is an independent claim addressed to a method of designing security for an IT system using a plurality of security subsystems and creating a functional technology diagram to document security requirements for an IT system. Claim 2 provides that the second system has a component using subsystems for identifying security properties. Claims 3, 5, 6, 12, 13, 14, and 15 provide that the framework use standard criteria. Claims 4 and 10 provide for documentation of the solution and assumptions of the framework. Claims 8 and 9 rank threats to the designed system. Claim 11 claims the process of developing integrity assurance requirements for the IT system. Claim 16 claims that certain steps of the developing a secure solution are performed by security subsystems.

In response to the Examiner's final rejection of the claims, Applicants traverse. The Examiner fails to present a prima facie case of obviousness under 35 U.S.C. §103(a). Applicants further assert that the invention of claim 7 is within statutory subject matter of 35 U.S.C. §101. Claims 1-16 are pending.

The Rejection of Claims 1-7 and 10-16 under 35 U.S.C. §103(a) over Bowman-Amuah '364, Alsberg '572, and Perona '809

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art references when combined must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. In re Vaeck, 947 F.2d 488, (Fed. Cir. 1991).

Applicants claims a methodology framework for designing security into an IT system. An important aspect is that security is designed into an IT system using this framework. The independent claims have five elements or five systems: (1) a first system identifies security threats; (2) the second system determines the security properties and functions of the IT system in terms of at least three subsystems: (2a) an audit, (2b) an integrity, and (2c) an information control

AFTER FINAL GROUP ART 2135

subsystem; (3) the third system allocates security properties to components of the IT system based on the functions derived from the subsystems of the second system; (4) the fourth system further allocates security properties to components of the IT system and identifies functional requirements for the components in terms of the Common Criteria, an international standard of security criteria for IT architectures; and (5) the fifth system documents the security requirements.

The Examiner rejected claims 1-7 and 10-16 under 35 U.S.C. §103(a) as being unpatentable over Bowman-Amuah '364, Alsberg '572, and Perona '809. The Examiner asserts that Bowman-Amuah '364 discloses a system and method for building systems in a development architecture framework wherein security is integrated into the solution. The Examiner admits that Bowman-Amuah '364 does not disclose the security subsystems, i.e., the audit subsystem, the integrity subsystem, and the information flow control subsystem of the second system; nor, the Examiner also admits, does Bowman-Amuah '364 disclose using a baseline of a security model comprising a plurality of interrelated and interdependent security subsystems. The Examiner proposes to modify Bowman-Amuah '364 with the teachings of Alsberg '572 which disclose a protector device allegedly having an audit subsystem, integrity subsystem, and information control subsystem. The Examiner further relies on Perona '809 as a system that performs rule checks by determining if there are licensing and source restrictions between the operating system, the modules, and the application software. The Examiner reasons that the modules of Perona '809 that check on licensing and source restrictions include security properties in terms of a plurality of interconnected and interdependent security subsystems, and that one of skill in the art would be motivated to combine the two or three references.

The Examiner must first establish that there must some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine reference teachings. In this case, the Examiner has failed to establish an objective basis for the motivation to combine the references. Here, the Examiner, rather than the references, provides the motivation for the alleged combination; the Examiner simply states that one of ordinary skill in the art would have been motivated to [include audit subsystem integrity subsystems, and information flow control subsystems] because auditing potentially sensitive

AFTER FINAL GROUP ART 2135

material, integrity subsystems, and controlling the information flow would increase the security of the system. The Examiner does not point to any suggestion within Bowman-Amuah '364 or Alsberg '572 themselves; the Examiner does not rely on any objective and independent source for the motivation. The motivation for the alleged combination proffered by the Examiner comes solely from the Examiner herself having the benefit of Applicants' teachings. Similarly, with respect to the motivation or suggestion for the combination of Bowman-Amuah '364 with Perona '809, the Examiner simply states that "one of ordinary skill in the art would have been motivated to [create a plurality of interconnected and interdependent security subsystems as in Perona '809 in the system of Bowman-Amuah '364] because it would enable higher levels of security. Again, neither Perona '809 nor Bowman-Amuah '364 nor any objective independent source provides any motivation or suggestion for the combination.

Merely stating that one of ordinary skill in the art would combine the references because the combination would make a more secure IT system does not sustain a prima facie case of obviousness. Applicants are aware that the MPEP states that the "strongest rationale for combining references is a recognition, expressly or impliedly in the prior art or drawn from a convincing line of reasoning based on established scientific principles or legal precedent, that some advantage or expected beneficial result would have been produced by their combination." MPEP 2144. Note, however, that the advantage or expected beneficial result must be expressly or implied in the prior art or derived from an objective independent source. Neither reference proposes integrating an audit subsystem into the design framework of a secure IT system. Bowman-Amuah '364 specifically teaches that the auditing function of the IT should be independent: Bowman-Amuah '364 briefly mentions the need for security audits for the development architecture framework but merely states that audits can be done by an **external body specializing in security in the form of interviews, architecture and code reviews**, and automated tool assessment. (Bowman-Amuah '364 at column 18, lines 60-63). Alsberg '572 also specifically teaches that the auditing function should be independent and remote (see below). Neither reference expressly or impliedly suggests the combination or that the advantage or benefit posited by the Examiner will result from their combination; instead both references teach that the audit subsystems should be remote and independent. The Examiner further fails to set

AFTER FINAL GROUP ART 2135

forth established scientific principles or legal precedent that the advantage or expected beneficial result (a more secure IT system) will be produced by the combination of Bowman-Amuah '364 with Alsberg. Thus, on the first criteria to establish nonobviousness, the Examiner fails.

The second criteria to establish a prima facie case of obviousness is that there must be a reasonable expectation of success. A corollary to both the first and this second criteria is that the proposed modification cannot change the principle of operation of a reference. *In re Raitti*, 270 F.2d 810, 123 U.S.P.Q. 349 (CCPA 1959). Applicants assert that there is no reasonable expectation of success with the Examiner's proposed combination, i.e., to modify Alsberg '572 in the combination with Bowman-Amuah '364 actually destroys the principle of operation of Alsberg. One of the objects and overriding principles of Alsberg '572 is "to provide a security protection device for a computer which can be remote from both a user's terminal and the actual computer to be protected" Alsberg '572 at columns 2, lines 19-23. The protector device of Alsberg '572, also called security server, is specifically intended to be "independent from the host computer and terminals but connected to the computers and terminals" Alsberg '572 at column 4, lines 1-3. The Examiner's proposed combination of Bowman-Amuah '364 with Alsberg '572 destroys the independence and remoteness intended by Alsberg. Applicants further assert that the Examiner's alleged motivation to integrate security into the solution for the imagined combination cannot be suggested by the Alsberg '572 reference because Alsberg '572 teaches against an integrated and interconnected design. Alsberg '572 specifically states:

One technique of preventing undesirable access is to design software that is demonstrably secure. That is, to design software that can be convincingly demonstrated to prevent access by a user to certain unauthorized levels of information and to allow access to certain authorized levels of information. **The problem with this technique is that such software typically requires precise design of system functions and structures so that the resulting software is secure against state-of-the-art threats and can be demonstrated to be secure using state-of-the-art technology such as formal verification/proof technology.** In order to add such security to existing software, the architecture of the existing software would have to be significantly redesigned. The resemblance of the resulting secure software designed from the preexisting software would be very slight and **would typically destroy compatibility between uses of the existing software and the software which has been made secure.** Alsberg '572 at column 1, lines 17-35. (Emphasis added).

AFTER FINAL GROUP ART 2135

Applicants ask of the Examiner: how can there be a reasonable expectation of success if one of the references teaches against the use proposed by the Examiner? How can merely adding a secure server result in the design of IT system that starts with principles of security and a number of secure subsystems integrated into the design, as claimed? Applicants thus argue that the Examiner fails to satisfy the second criterion necessary create a prima facie case of obviousness - that of having a reasonable expectation of success.

The third criterion to establish a prima facie case of obviousness is that the references when combined must teach or suggest all the claim limitations. First off, Bowman-Amuah '364 does not teach a methodology framework for designing security into an IT system that starts and ends with security, as claimed. Bowman-Amuah '364 teaches an integrated development framework for building systems. Security management is only one management system of many taught by Bowman-Amuah '364: the other management systems include configuration management, release management, quality management, environment management, information management, problem management, program and project management, and system building - all these aspects determine the architecture of the system. The most detail that Bowman-Amuah '364 provides for security management is presented at column 49, line 65 through column 51, line 13. The security management system of Bowman-Amuah '364 deals mainly with preventing unauthorized access to the system, e.g., *intrusion detection, network assessment, platform security to minimize the opportunities for intruders ..., web-based access control, fraud services, mobile code security, e-mail, encryption, public key infrastructure, authentication system, and firewall*. Bowman-Amuah '364 further admits that the audit security subsystem or function is independent from the security management system, not an integral, interrelated and interconnected subsystem of security, as Applicants have claimed. The Examiner has further admitted that Bowman-Amuah '364 does not teach the integrity subsystem claimed by Applicants.

Alsberg also does not provide the integrity subsystem as claimed by Applicants. The Examiner cites Alsberg '572 at column 7, lines 1-10 to teach an integrity subsystem but here Alsberg '572 only talks about administrator activities within several modules to edit a data base, analyze the audit-trail, maintain status and control the system. Applicants do not see how these

AFTER FINAL GROUP ART 2135

administrator modules make up an integrity subsystem, and more particularly, Applicants assert that “reading and changing the security data base,” “monitoring current system status”, “analyzing the audit-trail storage” and “controlling system activity” is not the same as the claimed integrity subsystem. Attorney for Applicants has reviewed the specification to determine if the claimed integrity subsystem includes any elements disclosed by the Alsberg ‘572 reference. Attorney for Applications is aware, moreover, that limitations from the specification are not read into the claims, In re Van Geuns, 988 F.2d 1181, 26 U.S.P.Q.2d 1057 (Fed. Cir. 1993), but respectfully, the Examiner is not free to conform or recreate the prior art to read onto the claims where there is no suggestion that the prior art reference teaches the claimed limitation. In other words, Alsberg’s administrative functions and modules as described in column 7, lines 1-10 do not teach the claimed integrity subsystem. Therefore, the Examiner has also failed on the third rung of the ladder of sustaining a case of prima face obviousness based on the combination of Bowman-Amuah ‘364 with Alsberg.

Applicants traverse the rejection of independent claims 1 and 7 under 35 U.S.C. §103(a) based on the alleged combination of Bowman-Amuah ‘364, Alsberg ‘572 and Perona ‘809. The Examiner asserts that Perona ‘809 discloses a system having checks on licensing and source restrictions between software modules, applications, and operating systems. The Examiner reasons that the licensing and compatibility checks provide the claimed plurality of interconnected and interdependent security subsystems. Applicants contend that the alleged combination of Bowman-Amuah ‘364, Alsberg ‘572 and Perona ‘809 also fail to satisfy the third criterion of creating a prima facie case of obviousness because Perona ‘809 does not teach the interconnected and interdependent security subsystems as claimed.

Perona ‘809 is applicable to an open architecture software communication system such as between a computer, a satellite, a cell phone, and any other hardware and software component that will be added. Perona ‘809 provides rule checks between the platform, i.e., the hardware and operating system, the stored applications, and a plurality of stored modules. Each module is a separate library of software used by the application to execute a specific function to implement the application, e.g., a module may perform data encryption, a different module may perform signal processing, or protocol processing, or network communications planning, or signal

AFTER FINAL GROUP ART 2135

modulation, and so on. Every time a new platform or a new application or a new module is added to the open architecture software communications system, the two-way rule checks occur to ensure the software, the platform, and the modules are all licensed and compatible.

Despite the Examiner's assertions, Perona '809 does not teach a plurality of interrelated and interdependent security subsystems, i.e., Perona '809 does not teach the audit subsystem, an integrity subsystem and an information control subsystem, as claimed. Merely checking for licensing and compatibility does not create Applicants' claimed interdependent and interconnected audit, integrity, and information flow control security subsystems, and then assigning the details of these security subsystems to define the infrastructure, functions and properties of components of the system. Adding Perona '809 to any system will merely check to see if the hardware and software components are licensed and compatible with each - there is no mention of managing audits, integrity, and information control.

In view of the remarks above, Applicants respectfully request the Examiner to withdraw the rejection of claims 1-7 and 10-16 under 35 U.S.C. §103(a) over Bowman-Amuah '364, Alsberg '572, and Perona '809.

The Rejection of claims 8-9 Under 35 U.S.C. §103(a) over Bowman-Amuah '364, Alsberg '572 in view of Leighton '778

The Examiner repeated her rejection of claims 8-9 under 35 U.S.C. §103(a) under a combination of Bowman-Amuah '364 and Alsberg '572 in view of Leighton '778. The Examiner applies Bowman-Amuah '364 and Alsberg '572 as above and then applies Leighton '778 as a reference to rank the security levels and threats to the system. Applicants repeat their traversal. Applicants reiterate that Bowman-Amuah '364 teaches an integrated development architecture relying on many aspects, other than security, to create the architecture. Bowman-Amuah '364 does not use the interconnectedness and interdependence of at least three security subsystems to define the functions and the properties of the entire system. Alsberg '572 teaches against using the precise detail to design security, such as claimed by Applicants, into a host computer and its terminals because of changing technology; therefore, Alsberg '572 teaches that security functions are best handled by an external security server. Leighton '778 applies a ranking system to users

AFTER FINAL GROUP ART 2135

of a cryptosystem wherein communications are ciphered between ranked users of the system, i.e., one user may have a higher security clearance/level than another user. Leighton '778 ranks only those users for secret-key exchange wherein first, users can directly talk to one another and second the conversation between two users always takes place at the highest common level of security, see column 6, lines 44-47. Leighton '778 does not suggest applying a ranking of security threats to the subsystems of a software development system or to an overall information handling system, as claimed by Applicants. Threats to management of audits, integrity, and information flow control are not suggested or even mentioned by Leighton '778, let alone ranking these threats. Thus, with the Examiner's observation that Bowman-Amuah '364 does not rank security threats combined with the fact that Leighton '778 ranks only the security level of users on a cryptographic system, Applicants contend that the Examiner has failed to create a prima facie case of obviousness because first, the references do not suggest their combination. Even when combined, the references do not teach the ranking of security threats to a plurality of security subsystems, as claimed. Applicants respectfully request the Examiner to withdraw the rejection of claims 8 and 9 under 35 U.S.C. §103(a).

The Rejection of claim 7 under 35 U.S.C. §101

The Examiner rejected claim 7 under 35 U.S.C. §101 saying the method steps do not result in tangible subject matter that falls within the statutory classes of a "new and useful process, machine, manufacture, or composition of matter or any new and useful improvement thereof." Applicants have reread 35 U.S.C. §101 and nowhere are the words "tangible" or "tangibly" required for statutory subject matter. Attorney for Applicants is aware of and has read the *Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility* published in the Official Gazette on 22 November 2005. Respectfully, neither the Patent Office nor the Examiner is at liberty to create a new statutory requirement for subject matter where none exist.

Even so, tangible is defined as "possible to be treated as fact; real or concrete: tangible evidence, or possible to understand or realize: the tangible benefits of the plan" from <http://www.thefreedictionary.com/tangible>. In claim 7, Applicants claim a "method" that

AFTER FINAL GROUP ART 2135

identifies, determines, assigns, enumerates, develops, and creates at least one functional technology diagram that documents security requirements for an IT system. Applicants assert that in reading claim 7, one of ordinary skill in the art may understand and realize the steps of designing security for an IT system. Applicants further surmise that these method steps and the creation of a functional technology diagram that documents the security requirements for the IT system is every bit as tangible as a method of designing an integrated circuit and the resultant circuit diagram of the design. The claimed method and a diagram of documented security requirements, when the claim is viewed as a whole, is a useful, concrete, and tangible result - the result being a design of secure IT system in the context of several security subsystems. To be able to make, use, and sell such a method and a design is surely patentable subject matter under 35 U.S.C. §101.

Respectfully, if the Examiner maintains the rejection of claim 7 under 35 U.S.C. §101, Attorney for Applicants shift the burden onto the Examiner to show how the claimed method is not useful, concrete, and tangible.

Conclusion

In order to establish a prima facie case of obviousness, the proper inquiry is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination. The motivation for the combination must come from some objective basis, other than the Examiner's hindsight garnered from references. The references, moreover, must be combinable, that is the teachings in alleged combination must not destroy the principles of the references. Applicants maintain that the Examiner fails to present a prima facie case of obviousness because first, the references themselves do not suggest or teach their alleged combination. Second, there is no reasonable expectation of success of the combination because both Bowman-Amuah '364 and Alsberg '572 teach that audit security should be done independently and/or remotely, not with an audit subsystem that is interdependent and interconnected with other security subsystems. Third, the alleged combinations do not teach all the claim limitations: Alsberg '572 does not teach an integrity subsystem as claimed; and Perona '809 does not teach the interconnectness and interdependence of the security subsystems in

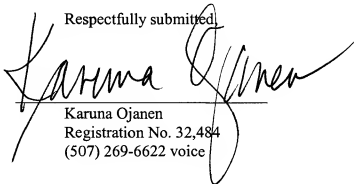
AFTER FINAL GROUP ART 2135

the information flow control subsystems are ranked. Merely ranking users' security as taught by Leighton '778 does not design security into an IT system.

Lastly, Applicants claim a novel and nonobvious framework and method to design a secure information handling system wherein audit, information control, and integrity security subsystems and the interconnectedness between them determine the properties, functions, infrastructure, components, and operations of the system. The method of the framework and the resultant diagram documenting the security requirements of the IT system, moreover, are real, understandable, tangible and within the statutory subject matter of 35 U.S.C. §101.

Attorney for Applicants thank the Examiner for her review of these remarks. Attorney for Applicants further invite the Examiner invited to telephone the Attorney listed below if she thinks it would expedite issuance of the patent.

Respectfully submitted,



Karuna Ojanen
Registration No. 32,484
(507) 269-6622 voice

Date: 25 September 2006

OLO - Ojanen Law Offices
2665 Riverside Lane, NE
Rochester, MN 55906-3456

54462
54462

PATENT TRADEMARK OFFICE